Department of Homeland Security Daily Open Source Infrastructure Report for 15 June 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports the National Transportation Safety Board is investigating why an engine on a Boeing 767 blew up during maintenance at Los Angeles International Airport. (See item 10)
- U.S. Immigration and Customs Enforcement agents and officers have apprehended approximately 2,179 criminal aliens, illegal alien gang members, fugitive aliens, and other immigration status violators as part of a nationwide interior immigration enforcement operation that began last month. (See item 27)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 13, Hawaii Channel* — **Explosion at Tesoro refinery damages liquid−asphalt tank.** An explosion in a tank at Tesoro Hawaii's oil refinery blew a hole in the tank used to make liquid asphalt, according to company spokesperson Jeanette Mukai. It happened at about 11:40 a.m. UTC Tuesday, June 13. After the hole was blown out the top of the tank, the tank was seen smoldering. Tesoro evacuated some people around the tank, but the plant continued operations. Source: http://www.thehawaiichannel.com/news/9365880/detail.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *June 14, CBS 3 (PA)* — **Fire breaks out in Chicago chemical plant, prompting business evacuation.** A 5−alarm fire erupted Wednesday, June 14, at the Universal Form Clamp Company industrial plant just west of Chicago, prompting officials to evacuate area businesses and call more than a dozen fire departments to help battle the smoky blaze. Four people were taken to Loyola University Medical Center with injuries.
   Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/14/AR2006061401047.html

3. *June 14, 6 ABC (PA)* — **Coast Guard closes Cape May Canal as result of diesel spill.** Over 600 gallons of diesel fuel leaked into the Sunrise Marina in Cape May, NJ, late Tuesday, June 13. The captain of a 91−foot yacht stopped there to fill up on drinking water and somehow the water was pumped into the fuel tank, which caused it to overflow. The spill forced the U.S. Coast Guard to close the Cape May Canal late Tuesday as the fuel spread into Cape May Harbor. As of Wednesday, June 14, the fuel had spread over a one square mile radius into the canal and back bay.
   Additional information: http://www.pressofatlanticcity.com/news/local/capemay/story/6436127p−6289883c.html
   Source: http://abclocal.go.com/wpvi/story?section=local&id=4268575

4. *June 13, Miami Herald* — **Florida market evacuated due to chemical smell.** A hazardous materials crew evacuated shoppers from the El Okey Market in Miami, FL, Tuesday, June 13, when people complained of a chemical smell in the air. Several people complained of difficulty breathing and nausea, but emergency workers could not locate what had caused the smell.
   Source: http://www.miami.com/mld/miamiherald/14810552.htm

[Return to top]

Defense Industrial Base Sector

5. *June 14, Government Accountability Office* — **GAO−06−709: Defense Management: Additional Measures to Reduce Corrosion of Prepositioned Military Assets Could Achieve Cost Savings (Report).** The military services store prepositioned stocks of equipment and material on ships and land in locations around the world to enable the rapid fielding of combat−ready forces. The Government Accountability Office's (GAO) prior work has shown that the readiness and safety of military equipment can be severely degraded by corrosion and that the Department of Defense (DoD) spends billions of dollars annually to address corrosion. GAO was asked to review the impact of corrosion on prepositioned assets. GAO’s specific objectives were to assess (1) the measures taken by the Army and the Marine Corps to reduce the impact of corrosion on prepositioned assets and (2) the availability of corrosion−related data to the Army and the Marine Corps to support corrosion prevention and mitigation efforts for prepositioned assets. To reduce the impact of corrosion on prepositioned assets and support

additional corrosion prevention and mitigation efforts, GAO is recommending that the Army examine the feasibility of using temporary shelters to store land−based prepositioned assets currently stored outdoors and that the Army and Marine Corps enhance their efforts to collect corrosion−related data on prepostioned assets. DoD concurred with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06709high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−709

6. *June 14, Government Accountability Office* — **GAO−06−693R: DoD Personnel Clearances: Questions and Answers for the Record Following the Second in a Series of Hearings on Fixing the Security Clearance Process (Correspondence).** In this report, the Government Accountability Office addresses three questions posed by the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. The Government Accountability Office (GAO) will continue to assess and monitor the Department of Defense's (DoD) personnel security clearance program, including DoD's progress in meeting the goals and objectives outlined in the governmentwide plan. At this time, GAO has no ongoing or future work that would assess whether the federal intelligence community is meeting the goals and objectives of the government's plan. GAO is currently reviewing the timeliness and completeness of DoD's and the Office of Personnel Management's processes used to determine whether industry personnel are eligible to hold a Top Secret clearance. GAO will report that information to the subcommittee this fall.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−693R

[Return to top]

Banking and Finance Sector

7. *June 14, KPTV (OR)* — **Oregon taxpayers may be victims of ID theft.** The Oregon Department of Revenue (ODR) is sending out letters warning more than 1,300 taxpayers that they could be the victims of identity theft. ODR says they found spyware on an agency computer that has been capturing and sending out private information to another computer over the Internet. The agency says social security numbers, names, and addresses were lost, but no financial or tax records were affected.
Source: http://www.kptv.com/global/story.asp?s=5027676&ClientType=Pr intable

8. *June 14, Computing (UK)* — **Phishing attacks against Europeans drop; U.S. banking customers suffer worse.** The number of phishing emails sent to American online banking customers in order to steal passwords and account details increased significantly last month, according to a survey by RSA Security released this week. The survey reveals that 62 percent of all phishing scams were aimed at U.S. banks and credit unions, while the number of identity fraud attacks against European and other financial institutions dropped. The majority of scams were launched by criminals using Internet service providers in the U.S., although overall the number of attacks launched from the U.S. decreased by 10 percent in May.
Source: http://www.computing.co.uk/computing/news/2158229/phishing−a ttacks−against

9. *June 13, Daily Record (NJ)* — **New Jersey man suspected in spree of banking scams.** A 28−year−old Rockaway man who was arrested on fraud charges for attempting to cash a $3,000

bogus check at a Commerce Bank in Montville, NJ, two weeks ago has pulled the same scam at branches across New Jersey, authorities said Monday, June 12. The scope of Gilberto Bras' scheme was revealed over the weekend, when the Barnegat Police Department discovered that Bras' description matched a suspect in a similar incident in the Shore community. Last August, a man presented a forged check for more than $3,000 at a Commerce Bank branch in the area, Barnegat Police said. Further investigation revealed that Bras had attempted to cash fraudulent checks in the same amount at five other Commerce Bank branches throughout New Jersey. He is suspected of stealing more than $27,000. Montville Police Sgt. Andrew Caggiano said Commerce Bank's security department was contacted following Bras' arrest on June 2.
Source: http://www.dailyrecord.com/apps/pbcs.dll/article?AID=/20060613/COMMUNITIES/606130320/1203/NEWS01

[Return to top]

Transportation and Border Security Sector

10. *June 14, Associated Press* — **Safety officials investigate airliner engine failure at LAX.** Safety officials are investigating why an engine on a Boeing 767 blew up during maintenance at Los Angeles International Airport (LAX) this month. The National Transportation Safety Board (NTSB) said Tuesday, June 13, one of the two engines on the American Airlines plane blew apart during a test run, sending pieces into the fuselage and the other engine, punching holes into the wings and scattering pieces as far as 3,000 feet away. No one was aboard the airplane during the accident and no one was hurt. The possibility, though, that an engine might explode in flight prompted NTSB investigators to spend four days at the accident scene. U.S.−made engines are regarded as extremely reliable, but there have been problems with fatigue cracking in certain engine parts.
Source: http://www.usatoday.com/travel/flights/2006−06−14−lax−engine_x.htm

11. *June 14, Associated Press* — **Northwest flight attendants to negotiate after judge approves two other deals.** Approval of new concessionary contracts for two Northwest Airlines worker unions adds new urgency to the carrier's talks with flight attendants −− a crucial last holdout group needed for the new deals to take effect. A bankruptcy court on Tuesday, June 13, approved nearly $550 million in concessions between Northwest Airlines and two of its unions representing pilots, baggage handlers and ground workers, but the airline will not realize the cost savings from the deals until it reaches agreement with the flight attendants. Each of the major unions negotiated a clause mandating that their concessions take effect only when the others do. Eighty percent of voting flight attendants rejected a proposed contract with Northwest last week that would have saved the company $195 million.
Source: http://www.usatoday.com/travel/flights/2006−06−14−northwest− talks_x.htm

12. *June 14, WNYC (NY)* — **Port Authority: NYC needs new airport.** Chairman of the Port Authority of New York and New Jersey Anthony Coscia, says New York and New Jersey need to start planning for a fourth airport now or there will be major problems ahead. He says it typically takes a city 12−15 years to get a new airport built. Earlier this month, Deputy Mayor Dan Doctoroff said congestion at John F Kennedy International Airport is "one of the biggest threats" to the city's continued growth and economy. At the same time, jet noise is becoming an increasingly thorny political problem.

Source: http://www.wnyc.org/news/articles/61208

13. *June 14, Aviation Now* — **House Committee directs FAA to accelerate crucial programs.** U.S. lawmakers are using the annual appropriations process to direct Federal Aviation Administration (FAA) to accelerate the introduction of runway safety and satellite navigation technology, and extra money is also being earmarked to speed FAA's hiring of safety inspectors. The House Appropriations Committee wants to boost funding for a runway safety system known as ASDE−X by $10 million in fiscal 2007, bringing the total for this program to $73.6 million. The extra money will enable FAA to "commission ASDE−X systems earlier than currently planned," the committee said in a report accompanying the fiscal 2007 transportation spending bill. The committee highlighted Chicago O'Hare as an airport where FAA must speed the deployment of ASDE−X. The contract tower program also received a funding boost from the Appropriations Committee, which recommended that $3.2 million be added to the Administration's request. This money will ensure funding for 12 new contract towers expected to enter the program in FY2007. House appropriators agreed to FAA's request for $18.2 million specifically to hire extra controllers to prepare for an expected retirement wave.
Source: http://www.aviationnow.com/avnow/news/channel_aviationdaily_story.jsp?id=news/FAAH06136.xml

14. *June 14, Government Accountability Office* — **GAO−06−864T: Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program (Testimony).** After the events of September 11, 2001, the Transportation Security Administration (TSA) assumed the function of passenger prescreening —or the matching of passenger information against terrorist watch lists to identify persons who should undergo additional security scrutiny—for domestic flights, which is currently performed by the air carriers. To do so, TSA has been developing Secure Flight. This testimony covers TSA's progress and challenges in (1) developing, managing, and overseeing Secure Flight; (2) coordinating with key stakeholders critical to program operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing impacts on passenger privacy and protecting passenger rights. A prior Government Accountability Office (GAO) report recommended that the Department of Homeland Security (DHS) direct TSA to take several actions to manage risks associated with Secure Flight's development, including finalizing system requirements, test plans, privacy and redress requirements, and program cost estimates, and establishing plans to obtain data needed to operate the system. DHS generally concurred with GAO's recommendations, but has not yet completed the actions it planned to take. TSA's re−baselining effort is reassessing program goals, requirements, and capabilities.
Highlights: http://www.gao.gov/highlights/d06864thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−864T

15. *May 15, Government Accountability Office* — **GAO−06−516: Mass Transit: Issues Related to Providing Dedicated Funding for the Washington Metropolitan Area Transit Authority (Report).** A regional panel estimated that the Washington Metropolitan Area Transit Authority (WMATA) −− Washington, DC's, transit system −− will have total budgetary shortfalls of $2.4 billion over 10 years. The panel and others have noted that WMATA's lack of a significant dedicated revenue source may affect its ability to keep the system in good working order. Proposed federal legislation would make $1.5 billion available to WMATA if the local governments established dedicated funding. This report addresses (1) the characteristics of

dedicated funding and its effects on transit agencies and governments; (2) how potential revenue sources compare in terms of stability, adequacy, and other factors; (3) major actions needed to establish dedicated funding for WMATA and the progress made to date; and (4) issues that dedicated funding poses for the region and WMATA. To address these issues, the Government Accountability Office (GAO) reviewed financial data for the nation's 25 largest transit agencies, interviewed officials from 6 transit agencies and from the state and local governments that support WMATA, and reviewed literature on the financing of mass transit. GAO provided a draft of this report to WMATA and the Department of Transportation for review. Officials from these agencies provided technical clarifications that were incorporated in the report, as appropriate.
Highlights: http://www.gao.gov/highlights/d06516high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−516

[Return to top]

Postal and Shipping Sector

16. *June 14, Associated Press* — **FedEx offers 'critical inventory' supply.** FedEx Corp. announced a new service Tuesday, June 13, for high−tech companies wanting equipment or replacement parts in small inventories around the country. FedEx officials said they expect the service called Critical Inventory Logistics to appeal to customers in telecommunications, medicine and other high−tech fields. The service will focus on small stocks of replacement parts, emergency equipment and other items, such as medical devices for surgical implants, at select Kinko's centers in major U.S. cities, FedEx said.
Source: http://biz.yahoo.com/ap/060613/fedex_inventory.html?.v=1

[Return to top]

Agriculture Sector

17. *June 14, Illinois Ag Connection* — **Emerald ash borer confirmed in Illinois.** A destructive, non−native pest that feasts on ash trees has been detected in northern Illinois. The Illinois Department of Agriculture announced Tuesday, June 13, that a beetle found in the yard of a Kane County home east of Lily Lake is an emerald ash borer (EAB). "A coalition of local, state and federal agencies, including the USDA's Animal and Plant Health Inspection Service, U.S. Forest Service and Illinois Department of Agriculture, has been preparing for this day the past two years," Agriculture Director Chuck Hartke said. "Now that the emerald ash borer has been confirmed within our borders, we'll activate our response plan and begin the task of eradicating it. The first step is to conduct an extensive survey of ash trees in the area to determine the extent of damage. The findings will help establish boundaries for a quarantine that will stop the movement of potentially contaminated wood and nursery products out of the area and prevent the spread of this pest." Since the emerald ash borer was first confirmed in the Midwest in the summer of 2002, more than 20 million ash trees are dead or dying.
EAB information: http://www.emeraldashborer.info/
Source: http://www.illinoisagconnection.com/story−state.cfm?Id=517&y r=2006

18. *June 13, Animal and Plant Health Inspection Service* — **Potato cyst nematode traced to single Idaho field.** Scientists looking for evidence of potato cyst nematode (PCN) in Idaho Tuesday, June 13, confirmed the presence of the pest in one eastern Idaho field. The cysts were discovered in soil samples collected by the U.S. Department of Agriculture's Animal and Plant Health Inspection Service and the Idaho State Department of Agriculture. The soil was collected as part of the investigation into the April 19, detection of the pest, which was found in routine samples taken at a potato grading station in Idaho. The nematode can reduce the yield of potatoes and other crops. There is no sign that the quality of tubers grown in Idaho has been affected. The soil samples that tested positive for PCN were collected from a 45−acre field located in northern Bingham County, south of Idaho Falls. Production in the area is for fresh market and processed potatoes, not seed potatoes.
PCN information: http://plpnemweb.ucdavis.edu/Nemaplex/Taxadata/G053s2.htm
Source: http://www.aphis.usda.gov/newsroom/content/2006/06/pcnematod e.shtml

19. *June 13, Animal and Plant Health Inspection Service* — **Adding Namibia to the list of regions free of foot−and−mouth disease proposed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is proposing to amend its current regulations by adding Namibia, except for the region north of the Veterinary Cordon Fence (VCF), to the list of regions considered free of foot−and−mouth disease (FMD) and adding the entire country to the list of regions free of rinderpest. APHIS has determined that the region of Namibia south of the VCF, is free from FMD, and the entire country is free of rinderpest. Under the proposal, Namibia would still be subject to certain import restrictions for FMD and rinderpest because of its proximity to or trading relationships with regions that are not free of these diseases. This proposed action would relieve FMD and rinderpest import restrictions on certain live animals and animal products from all regions of Namibia, except the region north of the VCF.
Source: http://www.aphis.usda.gov/newsroom/content/2006/06/fmdnamibi a.shtml

[Return to top]

Food Sector

20. *June 14, Associated Press* — **Man's death prompts state to investigate feed plant.** The state of Minnesota is investigating a fatal accident at a livestock feed processing plant that has received 12 safety violations since 2000. Juan Gregorio Perez Carrasco died Sunday, June 11, after falling into a pile of feed at Endres Processing. The Minnesota Occupational Safety and Health Administration (OSHA) is investigating to determine the cause and whether the plant violated any state−regulated labor laws, spokesperson James Honerman said. The agency investigated Endres Processing in 2000 when another employee died and four others were injured in an explosion, according to OSHA. Endres' second investigation began in 2001 after complaints about two fires at the plant, one of which injured an employee. During two routine checks in 2003 and 2004, the plant received eight violations in the first visit and one violation in the second for problems such as not installing railings on some stairways, not having eyewash solution available where needed and not monitoring air for carbon monoxide where forklifts are operated indoors.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/local/ 14814172.htm

21. *June 13, Food Safety and Inspection Service* — **Ham product recalled.** Thumann's Inc., a Carlstadt, NJ, importing firm, is voluntarily recalling approximately 664 pounds of boneless proscuitto ham that may contain Staphylococcus aureus enterotoxin, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, June 13. The proscuitto was produced on April 24, 2006. The product was shipped to distribution centers and retail establishments across the U.S. The problem was discovered through testing done by the Canadian Food Inspection Agency. FSIS has received no reports of illness associated with consumption of this product. Common symptoms of ingesting products with Staphylococcus aureus enterotoxin include nausea, vomiting, diarrhea and abdominal cramping.
Source: http://www.fsis.usda.gov/News_&_Events//Recall_018_2006_Rele ase/index.asp

[Return to top]

Water Sector

22. *June 14, KTEN (OK)* — **Colbert water situation getting worse.** Twenty−five hundred residents in Colbert, OK, are still under a water emergency. Residents are only allowed to use water for drinking, bathing and cooking. Tuesday, June 13, the mayor of Colbert, Randall Gorman, advised residents of the emergency situation. Gorman said that there has been a dramatic decrease in the water table. Colbert usually pumps 60−80 gallons of water a minute from their eight wells. Right now, they're averaging just 12 gallons−a−minute. There are only eight feet of water left in the aquifer the city is tapping into.
Source: http://www.kten.com/Global/story.asp?S=5026587

[Return to top]

Public Health Sector

23. *June 14, World Health Organization* — **Plague in the Democratic Republic of the Congo.** As of 13 June 2006, the World Health Organization has received reports of 100 deaths of suspected pneumonic plague, including 19 deaths in Ituri district, Oriental province. Suspected cases of bubonic plague have also been reported but the total number is not known at this time. Preliminary results from rapid diagnostic tests in the area confirm pneumonic plague. Additional laboratory analysis, including tests by culture, is ongoing on 18 samples. Ituri is known to be the most active focus of human plague worldwide, reporting around 1000 cases a year. The first cases in this outbreak occurred in a rural area, in the Zone de Santé of Linga, in mid−May. Isolation wards have been established to treat patients; close contacts are being traced and receiving chemoprophylaxis. However, control measures have been difficult to implement because of security concerns in the area.
Plague information: http://www.cdc.gov/ncidod/diseases/submenus/sub_plague.htm
Source: http://www.who.int/csr/don/2006_06_14/en/index.html

24. *June 13, Agence France−Presse* — **Death toll from polio in Namibia reaches ten.** Namibia's first outbreak of polio in more than a decade has left 10 people dead while the number of reported cases has increased to 53, the health ministry said. "We now have ten reported deaths and confirmed cases increased to 53 −− up from 34 cases last week," said Kalumbi Shangula,

permanent secretary of the health ministry. While the majority of cases were detected in and around the capital Windhoek, there have been recent reports of the outbreak reaching the central and northern regions, Shangula said. A mass vaccination program is due to start next week after the health ministry received a shipment of vaccines from the United Nations children's agency on Tuesday, June 13.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://news.yahoo.com/s/afp/20060613/hl_afp/namibiahealthpolio_060613204855;_ylt=Aq4qoACtVtwiP3DPG4Nz6puJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

25. *June 13, Voice of America* — **Counterfeit drugs endanger malaria victims.** Scientists are expressing alarm at a thriving counterfeit industry that is producing fake drugs to treat malaria. They worry the fake drugs are putting countless lives at risk, and could harm a highly effective anti−malaria drug. Last year, a 23−year−old Burmese man died after he took the drug, artesunate, to treat what was diagnosed as a routine case of malaria. The drug is normally very effective. The case was investigated by Oxford University's Paul Newton and colleagues. "I think the death, the very sad death, of the Burmese man is the tip of an iceberg," said Newton. The artesunate tablets that were used to treat the man were found to contain 20 percent of the amount of the active drug in a genuine pill. In the study, Newton and colleagues also reported the percentage of over−the−counter counterfeit pills containing no artesunate appears to have increased from 38 to 53 percent in Southeast Asia from 1999 through 2004. Experts are also concerned about a growing problem in sub−Saharan Africa, where artemisinin is frequently used as part of a combination therapy to treat malaria. Each year, the disease kills an estimated 1.5 million people, and infects another 300,000 to 500,000 people.
Study: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pmed.0030197
Source: http://www.voanews.com/english/2006−06−13−voa84.cfm

26. *June 12, Canadian Press* — **H5N1 avian flu viruses trigger worse disease in adult cells than in children.** Some avian influenza viruses, and particularly the H5N1 subtype, appear to prompt the human immune system to over−produce important pathogen−fighting chemicals called chemokines, triggering an exaggerated response that creates more damage than it fixes, a new study suggests. The study shows that at least with older versions of the H5N1 virus, this response −− referred to as a cytokine storm −− was significantly more acute in adults than children. The findings could help to explain why the 1997 outbreak of H5N1 was far more deadly for adults than children and why the infamous 1918 Spanish flu −− caused by the H1N1 subtype −− wreaked its greatest havoc on young adults. They could also offer clues to help in the design of therapies to treat infections caused by these viruses, by pinpointing the response that needs to be moderated to avoid this immune response tidal wave and the damage it inflicts.
Research abstract: http://www.journals.uchicago.edu/ucp/WebIntegrationServlet?call=ContentWeblet&url=http://www.journals.uchicago.edu/JID/journal/issues/v194n1/36098/36098.html?erFrom=5064606684298393160Guest&current_page=content
Source: http://www.cbc.ca/cp/health/060612/x061244.html

[Return to top]

Government Sector

27. *June 14, Department of Homeland Security* — **ICE apprehends criminal aliens, gang members, fugitives and other immigration violators.** Julie L. Myers, Assistant Secretary for U.S. Immigration and Customs Enforcement (ICE), on Wednesday, June 14, announced that ICE agents and officers have apprehended approximately 2,179 criminal aliens, illegal alien gang members, fugitive aliens, and other immigration status violators as part of a nationwide interior immigration enforcement operation that began last month. Dubbed "Operation Return to Sender," the initiative began on May 26, and concluded on June 13. Virtually every field office in the nation from ICE's Office of Investigations and ICE's Office of Detention and Removal Operations carried out the enforcement operation in conjunction with numerous state and local law enforcement agencies. Among the roughly 2,179 individuals arrested in the operation, roughly half had criminal records for crimes that ranged from sexual assault of a minor to assault with a deadly weapon, to abduction. In addition, roughly 367 of the arrested aliens were members or associates of violent street gangs, including Mara Salvatrucha or MS−13. The interior enforcement strategy complements the Department of Homeland Security's border security efforts by expanding existing efforts to target immigration violators inside this country, employers of illegal aliens, as well as the many criminal networks that support these activities.
Source: http://www.dhs.gov/dhspublic/display?content=5689

[Return to top]

Emergency Services Sector

28. *June 14, Associated Press* — **Hacker replaces Florida's emergency site during tropical storm.** Internet users logging onto Florida's public disaster Website Tuesday, June 13, for an update on Tropical Storm Alberto instead got an imposter page after a hacker broke into the site. Technicians quickly pulled the imposter page from the Floridadisaster.org Website and relocated the site to another server system.
Source: http://www.local6.com/news/9366455/detail.html

29. *June 14, Government Accountability Office* — **GAO−06−844T: Hurricanes Katrina and Rita Disaster Relief: Improper and Potentially Fraudulent Individual Assistance Payments Estimated to Be Between $600 Million and $1.4 Billion (Testimony).** Hurricanes Katrina and Rita destroyed homes and displaced millions of individuals. In the wake of these natural disasters, Federal Emergency Management Agency (FEMA) responded to the need to provide aid quickly through the Individuals and Households Program (IHP) program, which provides housing assistance, real and personal property assistance, and for other immediate, emergency needs. As of February 2006, FEMA made 2.6 million payments totaling over $6 billion. The Government Accountability Office's (GAO) testimony will (1) provide an estimate of improper and potentially fraudulent payments through February 2006 related to certain aspects of the disaster registrations, (2) identify whether improper and potentially fraudulent payments were made to registrants who were incarcerated at the time of the disaster, (3) identify whether FEMA improperly provided registrants with rental assistance payments at the same time it was paying for their lodging at hotels, and (4) review FEMA's accountability over debit cards and

controls over proper debit card usage. To estimate the magnitude of IHP payments made on the basis of invalid registrations, GAO selected a random statistical sample of 250 payments made to hurricanes Katrina and Rita registrants as of February 2006.
Highlights: http://www.gao.gov/highlights/d06844thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−844T

30. *June 13, Associated Press* — **Airport prepares for infectious disease outbreak.** About 125 people participated Tuesday, June 13, in an exercise dubbed "Spring Rain" at Connecticut's Bradley International Airport, putting into action the state's plans to respond to an infectious−disease outbreak at the airport. During the drill, some of the patients had trouble hearing an emergency medical technician as he tried to question them above the sounds of the air conditioner in the triage center. Officials from Bradley, the state Department of Public Health, the Connecticut Disaster Medical Assistance Team, the National Guard and others took note, learning how they could tweak the state's plan to handle an actual emergency. The drill dealt with a flu outbreak, but the protocols would be identical if the state was facing Ebola, smallpox, or any other contagious disease, said Leonard Guercia, the Department of Public Health's operations chief. The exercise was the result of two years of planning.
Source: http://hosted.ap.org/dynamic/stories/C/CT_BRADLEY_DRILL_CTOL−?SITE=CTNHR&SECTION=HOME&TEMPLATE=DEFAULT

31. *June 13, Associated Press* — **Wildfire brings hard lessons.** When the Hayman fire blackened 138,114 acres and destroyed 599 structures in 2002, it left behind more than smoldering tree trunks and charred earth. Colorado's largest recorded fire racked up a $42 million firefighting tab and a $75 million bill for water treatment, evacuation costs and rehabilitation projects. The Hayman dealt hard lessons, some leading to action: a) federal firefighting spending has risen from $1.38 billion in 2002 to $1.86 billion this year; b) the Colorado General Assembly this year established a $3.25 million wildfire preparedness fund to ensure that 10 fire trucks bought under Governor Bill Owens' 2002 order are staffed and ready; c) the Colorado Forest Service boosted its military surplus fire truck fleet to 138 from 133, and most have been fitted with better pumps and foam applicators; d) the state built a database of city, county, fire district, emergency medical and search and rescue resources to improve responses and orchestrated a series of mutual aid agreements among agencies; e) agencies now train and exercise by region; f) millions in federal homeland security dollars have been pumped into equipping and training rural departments.
Source: http://www.jacksonholestartrib.com/articles/2006/06/13/news/regional/a1d8b9c85a78669c8725718b007451b2.txt

32. *June 13, Sun Herald (MS)* — **Storm plans include Wal−Mart.** Hurricane Katrina demonstrated the ability of Wal−Mart, the world's largest retailer, to move in supplies, which explains why Wal−Mart had a seat at the table for an emergency planning session in Biloxi, MS, Monday, June 12. Wal−Mart representatives met with area mayors and first responders to ensure an organized response should another hurricane strike the coast. The representatives asked each locality for a list of contacts and emergency supplies that would be needed after a storm. Brian Thomas, who manages South Mississippi Wal−Marts, said the company has the largest trucking fleet in the United States. Wal−Mart is also working with the Salvation Army and American Red Cross to make sure needs are met at shelters and other facilities.
Source: http://www.sunherald.com/mld/thesunherald/news/special_packa

ges/renewal/long_beach/14804959.htm

33. *June 13, Times−Picayune (LA)* — **Red Cross: New Orleans' shelters unsafe.** The leader of the American Red Cross announced Monday, June 12, that New Orleans residents living in Federal Emergency Management Agency trailers will need to evacuate north of Interstate 12 if they want to stay in shelters managed by the humanitarian agency. Red Cross interim President Jack McGuire said the organization does not plan to staff the city's proposed shelters because they may not be the safest option and do not meet Red Cross requirements. The Red Cross does not set up shelters, but it manages shelters opened by the state and parishes, including city shelters in the past. The agency has been working closely with the state to identify shelters and how to accept people into them. The Red Cross also has reviewed the process the state will use to move people to the shelters, McGuire said. If other locations in the city are proposed as shelters, they will go through a vigorous review, Red Cross officials said. McGuire said engineers must evaluate potential shelters to consider potential risks beyond whether the building may take water during a storm.
Source: http://www.nola.com/news/t−p/neworleans/index.ssf?/base/news−5/115017921781230.xml&coll=1

34. *June 13, U.S. Air Force* — **Air Force to test new instrument for collecting hurricane data.** Air Force reservists from the 53rd Weather Reconnaissance Squadron's "Hurricane Hunters" began flying the year's first storm missions Saturday, June 10, into Tropical Storm Alberto. The crew will soon have a new instrument, called the Stepped Frequency Microwave Radiometer, which remotely measures surface winds. The radiometer will be tested in November and is expected to be approved for operational use next season. This will allow continuous and direct measurement of the winds on the ocean surface and provide the National Hurricane Center with much higher resolution data about storms at lower levels, where people and property are impacted.
Source: http://www.af.mil/news/story.asp?id=123021578

[Return to top]

Information Technology and Telecommunications Sector

35. *June 14, Security Focus* — **Cisco VPN3K/ASA WebVPN Clientless Mode cross−site scripting vulnerability.** Cisco VPN 3000 Series Concentrators and ASA 5500 Series Adaptive Security Appliances (ASA) are prone to cross−site scripting attacks via the WebVPN Clientless Mode. Analysis: The issue is due to insufficient sanitization of HTML and script code from error messages that are displayed to users. This vulnerability could result in execution of attacker supplied HTML and script code in the session of a victim user. In the worst case scenario, the attacker could gain unauthorized access to the VPN by stealing the Web VPN session cookie.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18419/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18419/references

36. *June 14, Government Accountability Office* — **GAO−06−866T: Veterans Affairs:**

Leadership Needed to Address Information Security Weaknesses and Privacy Issues (Testimony). The recent information security breach at the Department of Veterans Affairs (VA), in which personal data on millions of veterans were compromised, has highlighted the importance of the department's security weaknesses, as well as the ability of federal agencies to protect personal information. Robust federal security programs are critically important to properly protect this information and the privacy of individuals. The Government Accountability Office (GAO) was asked to testify on VA's information security program, ways that agencies can prevent improper disclosures of personal information, and issues concerning notifications of privacy breaches. In preparing this testimony, GAO drew on its previous reports and testimonies, as well as on expert opinion provided in congressional testimony and other sources. To ensure that security and privacy issues are adequately addressed, GAO has made recommendations previously to VA and other agencies on implementing federal privacy and security laws. In addition, GAO has previously testified that in considering security breach notification legislation, the Congress should consider setting specific reporting requirements for agencies.
Highlights: http://www.gao.gov/highlights/d06866thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−866T

37. *June 13, U.S. Computer Emergency Readiness Team* — **US−CERT Technical Cyber Security Alert TA06−164A: Microsoft Windows, Internet Explorer, Media Player, Word, PowerPoint, and Exchange Vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Word, PowerPoint, Media Player, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial−of−service on a vulnerable system. Systems affected: Microsoft Windows; Microsoft Windows Media Player; Microsoft Internet Explorer; Microsoft PowerPoint for Windows and Mac OS X; Microsoft Word for Windows; Microsoft Office; Microsoft Works Suite; Microsoft Exchange Server Outlook Web Access. For more complete information, refer to the Microsoft Security Bulletin Summary for June 2006.
Solution: Apply updates: Microsoft has provided updates for these vulnerabilities in the Microsoft Security Bulletin Summary for June 2006:
http://www.microsoft.com/technet/security/bulletin/ms06−jun. mspx
Microsoft Windows updates are available on the Microsoft Update site:
https://update.microsoft.com/microsoftupdate/v6/muoptdefault
.aspx?ln=en&returnurl=https://update.microsoft.com/microsoft
update/v6/default.aspx?ln=en−us
Workarounds: Please see the following Vulnerability Notes for workarounds:
http://www.kb.cert.org/vuls/byid?searchview&query=ms06−june
Source: http://www.uscert.gov/cas/techalerts/TA06−164A.html

38. *June 13, Associated Press* — **Japanese virus spreading concern.** A computer virus that targets the popular file−sharing program Winny isn't the most destructive bug or even the most widespread. But it's the most talked about in Japan as it generates headline after headline, month after month. The malware, called Antinny, finds random files on Winny users' PCs and makes them available on the file−sharing network. So far, the data leaked have been varied and plentiful: passwords for restricted areas at airports, police investigations, customer information, sales reports, staff lists. The constantly updated virus seems to have spared no one −− airlines,

local police forces, mobile phone companies, the National Defense Agency. Antinny also may have the dubious distinction of being the first virus to exploit the nature of file−sharing itself −− in Japan, if not in the world, said Mamoru Saito of Telecom Information Sharing and Analysis Center Japan. Other viruses and spyware are often found on such networks, though none appears to take advantage of the underlying technology to spread personal data. And while Antinny's writers seem to be limiting themselves to Japanese file−sharing software for now, he said, the code theoretically could be modified to attack other file−sharing networks such as Gnutella and BitTorrent.
Source: http://www.cnn.com/2006/TECH/internet/06/13/japan.winny.ap/i ndex.html

39. *June 13, Information Week* — **Yahoo Mail worm may be first of many as Ajax proliferates.** The Yamanner worm that infested Yahoo Mail was quickly countered by making a change to the Internet servers that administer Yahoo's popular e−mail program. Nevertheless, over a 36−hour period, the world got a glimpse of what's in store for it unless stricter measures are followed in building Web applications. Yahoo Mail relied on a JavaScript function in connection with uploading images from a message to their mail server. JavaScript is a key component of Ajax, a set of technologies that is being used more and more frequently for Web applications. "This kind of worm shouldn't be a surprise to anyone. We can expect to continue to see viruses" as long as Websites and enterprises are implementing Ajax applications without understanding their vulnerabilities, said David Wagner, assistant professor of computer science at the University of California at Berkeley. Without careful, designed−in security, Web applications using Ajax will open many additional doors to malicious code writers. "The problem isn't that Yahoo is incompetent. The problem is that filtering JavaScript to make it safe is very, very hard," said Wagner. Not only is hard to defend against misuse of JavaScript, it's easy for skilled hackers to find the openings.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=189400799&subSection=Breaking+News

40. *June 13, IDG News Service* — **Internet pioneers warn of VoIP wiretap danger.** U.S. government efforts to require most voice−over−IP (VoIP) providers to permit law enforcement agencies to wiretap phone calls could introduce new security problems to the Internet, a group of Internet security experts said Tuesday, June 13. A Federal Communications Commission rule requiring providers to allow wiretapping by May 2007 would either require a massive re−engineering of the Internet or introduce broad cybersecurity risks, said authors of a new study released by the Information Technology Association of America (ITAA), an IT vendor trade group. In addition, the requirements would stall Internet innovations in the U.S. by adding hundreds of thousands of dollars in setup and maintenance costs to providers and potentially to other Internet applications that provide voice services, including instant messaging and online games, said the study.
ITAA study: http://www.itaa.org/news/docs/CALEAVOIPreport.pdf
Source: http://www.computerworld.com/action/article.do?command=viewA rticleBasic&articleId=9001158

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 − Symantec products vulnerable to buffer overflow:
http://www.kb.cert.org/vuls/id/4049100

Symantec Advisory SYM06−010 − Symantec Client Security and Symantec AntiVirus Elevation of Privilege:
http://securityresponse.symantec.com/avcenter/security/Conte nt/2006.05.25.htmll

US−CERT will advise as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 38566 (−−−), 6881 (bittorrent), 135 (epmap), 24232 (−−−), 25 (smtp), 4672 (eMule), 139 (netbios−ssn), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer